Order No. 938P

Distributed by:

Defense Threat Reduction Agency
DTIRP Outreach Program
8725 John J. Kingman Road, MSC 6201
Fort Belvoir, VA 22060-6201
1.800.419.2899
Email: dtirpoutreach@dtra.mil
Web: http://dtirp.dtra.mil

Your Facility's Public Information and Security Countermeasures Plan

Order No. 938P
March 2004

This pamphlet was prepared by the Defense Treaty Inspection Readiness Program (DTIRP) to increase **Readiness Through Awareness** within the U.S. Government and defense contractor community. Additional copies of this pamphlet, as well as other information about arms control treaties and the application of security countermeasures, are available through the DTIRP Outreach Program.

March 2004

Prepared for:
Defense Threat Reduction Agency
DTIRP Outreach Program
8725 John J. Kingman Road, MSC 6201
Fort Belvoir, VA 22060-6201

From the DTIRP Outreach series: Order No. 938P

TABLE OF CONTENTS

INTRODUCTION

This pamphlet examines the impact of publicly available information on a facility's arms control security countermeasures plan. Specifically, the pamphlet identifies methods by which arms control inspectors could obtain open source data concerning a facility. After reading this pamphlet, site and facility managers should be able to locate and identify publicly available facility information and create a public information inventory and monitoring system. This will help maintain consistency in facility information release and is useful in assessing the impact of open source data on a facility's arms control security countermeasures plan.

To understand this impact, you must be aware of the potentially intrusive nature of arms control verification measures and current provisions for on-site inspections. Equally important, you must understand how to survey, identify, and monitor open source data related to national security, proprietary, and other critical information from the viewpoint of the arms control inspector. The results will benefit site preparation for arms control verification activities and will have a much broader application in protecting critical information.

ARMS CONTROL VERIFICATION

Recent and emerging arms control treaties and agreements feature increasingly intrusive verification measures. These measures include procedures and activities allowed by the treaty and are used by inspectors to collect the data necessary for States Parties to determine compliance. Examples of such measures include data declarations, on-site inspection, and aerial observation.

Data declarations are used as an information baseline, which is the heart of all arms control agreements seeking to limit armaments or activities. The declarations establish the benchmark levels for each State Party and present the levels available for monitoring, observation, or reduction/elimination. Verification regimes established under recent and emerging arms control treaties provide for routine declarations of activities and stockpiles to an international body.

On-site inspections involve the treaty's implementing authority assigning and sending international inspectors to collect firsthand information. This information is necessary to verify the contents of a facility's data declaration or otherwise determine a facility's compliance with the treaty or agreement. With each new arms control agreement, the information collected and types of activities inspectors may employ to verify data declarations or to support a compliance judgment have grown increasingly intrusive and pervasive. They also focus increasingly on defense and commercial industrial processes. They have the potential to impact a large number of U.S. facilities, including fertilizer plants under the Chemical Weapons Convention (CWC), pharmaceutical companies under the CWC and the Biological Weapons Convention (BWC), and mining and construction under the Comprehensive Nuclear Test-Ban Treaty (CTBT).

Although international organizations overseeing treaty implementation efforts do not employ direct collection activities to provide facility information to inspectors, inspectors can use the Internet or other open source information media to gather relevant information about an inspection site prior to deployment. Site and facility managers must assume international inspectors will be armed with all publicly available information concerning their facility's operations, layout, and structure. Therefore, site and facility managers must ensure their security countermeasures plan continues to protect critical information in the most efficient and cost-effective manner.

The increased intrusiveness of inspection activities, coupled with the technological revolution evidenced by the Internet, has created substantial new security challenges. A site or facility manager must understand and adapt to these new challenges.

PUBLIC INFORMATION & YOUR FACILITY'S SECURITY COUNTERMEASURES PLAN

Types and Sources of Publicly Available Information

Public information is open source materials readily available to any individual, foreign or domestic, through a variety of media. Site and facility managers should understand that a variety of information concerning their facility may be available to the public, and therefore to arms control inspectors. Examples of publicly available information that may be of interest and of value to inspectors include: facility records; promotional literature and marketing material (e.g., company brochures, press releases); government publications; industry association newsletters; newspapers and magazines; and trade journals. Official government documents in the public domain also can provide valuable information. For example, Environmental Protection Agency (EPA) and Occupational Safety and Health Administration (OSHA) reports on violations of federal regulations, court records associated with lawsuits filed against companies for accidents or safety incidents, environmental impact statements, and shipping manifests for the transport of hazardous material required by the Department of Transportation (DOT) are available to the public. Even facility blueprints registered with a local government office often are available to the public upon request and can provide information about activities occurring at a facility. Together, such materials can provide considerable background about a facility's history, processes, operations, personnel, contractual relationships, technical capabilities, geographical layout, and physical characteristics.

In the past, the main sources of public information included newspapers, academic journals, and commercial periodicals. In today's modern technological age, the most common medium for obtaining such information is the Internet. The advent of the Internet has significantly reduced the amount of time and effort required to obtain public information. Essentially, anyone in the world with access to a browser-equipped computer can obtain public information in a matter of seconds.

Although much of the information contained on the Internet is unofficial and unverifiable, the Internet has become a marketing venue, a communication tool, and an information warehouse. Companies and facilities often use web pages to tout new products and unique operations to attract clients. The businesses and sites also may use web pages to connect various geographical offices to provide a means for scientists, professionals, and other employees to exchange data and information. Scientific data or reports written by the employees may be posted on web pages to facilitate interoffice and scientific exchange. Specific technical data, Material Safety Data Sheets (MSDS), and health and safety guidelines are common on these types of pages. Even Chemical Abstracts Service (CAS) registry numbers—which can support the identification of specific types of chemicals used or produced by a facility—may be found online. Internet users also can find company newsletters, journals, annual reports, shareholder information, and other pamphlets or marketing material on a company's homepage. Finally, by reviewing listed client web pages, analysts can use product information to ascertain the possible presence of chemical, biological, nuclear, or other items of interest.

To augment data found on company pages, researchers can use online local newspaper archives to search for facility-related reports and documents. These reports and documents can include information about environmental concerns, EPA and OSHA violations and inspections, personnel promotions, and scientific achievements associated with the facility. Often these stories will contain chemical names, locations, personnel data, and other information regarding facility activities. Additional online information that may assist an arms control inspector in assembling a mosaic of facility information include: federal, state, and local government records; police and fire department archives of environmental or safety hazards; contract announcements; information posted on Chamber of Commerce web sites; industry newsletters; scientific journals or magazines; investment guides; judicial proceedings, court docket information and other legal documents; Federal Register information; and federal or state agency pages. Online patent information can provide clues about operations and processes at a facility.

The Internet provides an easy and cost-effective medium to obtain information. Site and facility managers must be aware that arms control inspectors, armed with sufficient Internet know-how, can obtain a wealth of information about their facility in preparation for an inspection. The knowledge possessed by inspectors could pose significant challenges to traditional operations security countermeasures considerations, and may require retooling of an existing facility security countermeasures plan. Facility-specific information can be manipulated to serve the interests of States Parties during arms control verification activities. For example, under a CWC challenge inspection scenario, such data may suggest unauthorized or non-compliant activity.

What to Do?

There is very little a facility can do to redact information once it enters the open source. However, this does not mean you cannot use this information to your advantage. Site and facility managers should identify and then incorporate open source indicators of critical information into their security countermeasures plan. This will accomplish a number of objectives. First, a thorough review of open source information will increase your awareness. Second, you will be able to spot vulnerabilities and plug holes in your existing security countermeasures plan by reallocating your resources to protect critical indicators not already detectable in open source material. Using this methodology, you will be able to modify your security countermeasures plan's focus to protect critical information. As stated previously, there is no need to protect information commonly accessible through open source means. Knowing what information is available in the open source will assist in your labor and time allocations when implementing your security countermeasures plan.

Restructuring your security countermeasures plan to account for open source information requires some planning. The first step toward protecting your critical information in an efficient and cost-effective manner is to understand the information an inspector may possess (i.e., the facility data declaration and public information). Site and facility managers must assume inspectors are coming to their facility armed with all available public information and/or with the specific knowledge derived from your facility's data declaration. Taken together, these two knowledge bases can provide a wealth of information regarding facility operations unrelated to the object and purpose of the inspection.

You probably are already familiar with your facility's data declaration. Open source data regarding your facility will require some research and analytical efforts on your part. For example, you must identify, gather, and analyze information from multiple sources, as an inspector would. Using this information, you may then identify critical indicators of sensitive operations and processes by developing a mosaic—that is, assembling pieces of information derived from a number of sources to present a picture of the whole, much like a jigsaw puzzle. Using the mosaic, you must adapt your security countermeasures plan to protect sensitive operations and processes, without wasting time and money protecting information already widely available through open sources. This step is a critical point in developing a cost-effective security countermeasures plan. Protecting widely available information not only wastes time and money, but also draws the unnecessary attention of inspectors to sensitive operations or processes unrelated to the inspection mandate. You must develop an open source inventory and monitoring system to ensure you are up-to-date on publicly available information concerning your facility. If you prepare for an inspection employing the above methodology, your countermeasures plan will capture and protect national security and proprietary information in an efficient, cost-effective manner.

Due to the variety and diversity of facility security concerns, it is impossible to tailor a public information survey applicable to all inspectable facilities. There are a myriad of methods through which open source information is accessible. Understanding some of the basics of open source data collection will increase your awareness about how to apply an open source search to your facility. This understanding also will assist you in developing your own site-specific, open source data review process.

The first step is to decide upon functional responsibilities for the review. Although this effort need not be manpower intensive, several individuals will be necessary for consultation and advice throughout the review process. Some planning will be necessary to establish lines of communication to personnel familiar with marketing and advertising, public affairs, information systems, legal, and scientific departments of the facility. These individuals will be critical in ensuring the review is comprehensive and accurate. They also are useful at the onset of the review because they are most familiar with the avenues by which the facility provides information to the public at large, as well as to specialized audiences. Most importantly, the open source reviewer(s) will require lines of communication to personnel familiar with the national security and proprietary programs and operations of the facility. These individuals will be essential in providing advice on critical indicators of sensitive operations and processes. Early in the review, you will need upper management to verify a common definition of "proprietary information." As a rule, proprietary information is any information you would not want released to a competitor. Establishing a clear definition is necessary to focus effort during the review process.

There is no set pattern for reviewing open source information applicable to every facility. Typically, the search should begin with information released directly by the company, as this information is most easily controlled by the facility. This information also will likely be the first type accessed by individuals researching your facility. The self-review should include newsletters, journals, annual reports, budget data, contract announcements, company histories, marketing programs, and other internally-generated information. Marketing and advertising personnel can provide guidance concerning the types, locations, and availability of marketing data to the public. Public relations personnel can assist in identifying brochures, pamphlets, outreach programs, newsletters, employee speeches, press releases, and other direct efforts of the facility to provide information to the public. Information systems personnel can assist in identifying all files accessible to the public via the company's home page. They also can provide information concerning the publishing of facility data through list servers, online bulletin boards, and accessibility of the facility's Intranet via the Internet. The specific items to look for when reviewing documents are any reference to national security, Department of Defense or other government agency programs, and proprietary information.

The second step is to review specific web resources. The review should begin with an analysis of information found on company web pages. It should include any operations- or process-specific information; raw material, safety, or security information; or any other specific facility data found on the publicly accessible facility web site. Often, the most detailed and reliable source for a facility's open source data is its own web page.

Once you have conducted an inventory of information found on the company or facility web site, you can initiate a search for information on the Internet originating from external sources. There are a vast number of sites requiring review during this phase of the public information assessment. This portion of the assessment may be time-consuming, but it is arguably the most important element of the public information assessment due to the variety of information retrievable about the facility. To accomplish this review, the assessor(s) must be familiar with the operation of the Internet. They must understand the fundamentals of search engines, online database searches, and the manner in which information is organized and retrieved online.

The first task in conducting this portion of the Internet assessment is to develop a list of security and facility-related search keywords. The keyword list may grow quite lengthy, depending upon the nature and scope of national security and proprietary activity on-site. The keyword list should contain words associated with the facility such as company and business division names, colloquialisms, operational or process titles, products, building names, chemicals or other raw materials, publications, staff names, and any other site-specific information. A starting point for the list construction may be "metatag" information embedded on the company web site pages (information management and company web design personnel will have this information). Using this list of keywords, a user should methodically search the Internet for facility and operational specific information, using every keyword on each search engine and directory. There are many search engines and directories available online and you may have your own favorites.

The following search engines are a good place to begin this assessment:

- **Altavista** - [http://www.altavista.com]
- **AOL Netfinder** - [http://search.aol.com]
- **Ask Jeeves** - [http://www.ask.com]
- **Brittanica Internet Guide** - [http://www.ebig.com]
- **Dogpile** - [http://www.dogpile.com]
- **Excite** - [http://www.excite.com]
- **GoTo.com** - [http://www.go2online.com]
- **Google** - [http://www.google.com]
- **Hotbot** - [http://www.hotbot.com]
- **Infoseek** - [http://www.infoseek.com]
- **LookSmart** - [http://www.looksmart.com]
- **Lycos** - [http://www.lycos.com]
- **MetaFind** - [http://www.metafind.com]
- **MSN Search** - [http://search.msn.com]
- **Northern Light** - [http://www.northernlight.com]
- **Profusion** - [http://www.profusion.com]
- **Search** - [http://www.search.com]
- **TerraServer** - [http://www.terraserver.com]
- **WebCrawler** - [http://www.webcrawler.com]
- **Yahoo!** - [http://www.yahoo.com]

The sites listed above are not a comprehensive listing of search engines or meta-searchers on the Internet, but do serve as a good basis upon which to begin your open source information assessment. A majority of the search-locatable content on the Internet is accessible using these search engines and directories. During your review, remember to approach all information with an open mind. Information may come from a variety of sources, including those not normally relied upon to acquire company-specific information. As mentioned previously, client pages, government pages, non-government organization pages, contract announcements, newspapers, legal documents, personnel information and phone numbers, industry-related pages, and science-related pages are useful tools in gathering open source data related to a specific facility or process.

Once the information has been collected, the actual assessment element of the process begins with the organization and analysis of open source data. You should analyze the data, including information obtained from the web and elsewhere, with the eye of an inspector or outside researcher. You should use site-specific national security and proprietary information to focus this analysis. For example, take a sensitive program you have on-site requiring protection. Analyze each data source carefully for information regarding the specific program, and compile a list of open source information found. Using the list of open source data, develop a matrix or description of the project. Present the project matrix or description to the project manager, chemist, or engineer responsible for oversight of the project for an accuracy assessment. This evaluation will enable you to rank or assess the completeness of your mosaic of facility operations. Applying this approach to all sensitive operations on-site will enable you to complete an assessment of publicly available information about your facility. This picture will provide the “worst-case” scenario for facility security and site preparation personnel concerning information an inspector or visitor may possess about your facility prior to their arrival on-site.

As you can see, this assessment element has a wide-range of security applications outside of the arms control verification arena. Open source data assessment is particularly useful for an arms control security countermeasures plan. Using the matrices or project descriptions derived from the open source data review, the facility security countermeasures plan can be modified. These documents will facilitate identification of security gaps and enable the readjustment of the security plan to plug gaps or use facility resources more effectively. The most important contribution the assessment provides is the ability to narrow the security countermeasures plan to protect only sensitive information unrelated to the object and purpose of the inspection. The plan will help facility management to weigh the balance between available resources and necessity during site preparation activities for arms control inspections.

Once you have applied the data review to your facility security countermeasures plan, you can use the open source data review as the basis for subsequent assessments. The plan provides site and facility managers with the background necessary for analysis of future information produced by the facility concerning its operations. The plan also will enable managers to understand the impact of new information disseminated by the facility and others on the facility’s security countermeasures plan. When analyzed with reference to the specific requirements of an arms control verification regime, the open source data review will enable facility inspection response teams to prepare documents, buildings, and facility personnel to demonstrate compliance, while simultaneously protecting critical information.

CONCLUSION

This pamphlet has examined the impact of publicly available information on a facility's arms control security countermeasures plan and identified methods by which arms control inspectors may obtain open source materials concerning a facility.

To obtain additional information about any arms control treaties that potentially affect your facility, and the application of appropriate security countermeasures, contact the DTIRP Outreach Program Coordinator at 1-800-419-2899, your local Defense Security Service (DSS) Industrial Security Representative, or your government sponsor. Also see the list of related DTIRP products on the next page.

RELATED MATERIALS

407C Arms Control Treaties Information
CD-ROM

408P Arms Control Agreements Synopses
Pamphlet

410P Quick Reference Guide to
Arms Control Inspection Timelines
Pamphlet

907P DTIRP Arms Control Outreach Catalog
Pamphlet

908V Facility Protection Through Shrouding
Video

930C The Arms Control OPSEC Process
Automated CD-ROM

936V Verification Provisions—Point and Counterpoint
Video

942C DTIRP Outreach Products on CD
CD-ROM

950V The Technical Equipment Inspection (TEI) Process
Video

951V, 952V, 953V The Arms Control
Inspection Readiness Series
Video Trilogy

954T Why TEI?
Trifold Brochure

NOTES